

PROPOSED AMENDMENTS TO THE CLAIMS

Claims 1, 4-9, 13, 15, and 18-22 are pending in the subject application. It is proposed that each of claims 1, 6-9, 15, and 20 be amended as set forth herein. Upon entry of the proposed amendments, claims 1, 4-9, 13, 15, and 18-22 will remain pending. It is respectfully submitted that no new matter has been added by way of the proposed amendments. All claims that will be pending and under consideration in the present application upon entry of the proposed amendments are shown below. This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method performed by a client comprising:

storing a secret in a secure storage;

receiving a password challenge from a server; and

responsive to the password challenge, calling a secure password prompt routine which to execute a procedure, wherein the procedure comprises:
 - (1) accessing ~~accesses~~ the secret in the secure storage[.];
 - (2) generating ~~generates~~ an authentication graphic based on the secret[.]; and
 - (3) displays ~~rendering~~ a prompt asking a user for a password at a display device, the prompt including a request for a user to input a password and the authentication graphic, which ~~is~~ are visible to the user; wherein the secure password prompt routine displays ~~renders~~ the authentication graphic for all password challenges, ~~there being no~~

~~requirement of an association between the server and the authentication graphic.~~

2-3. (Cancelled)

4. (Previously Presented) The method of claim 1, further comprising making the authentication graphic known to the user so that the user can identify the authentication graphic on the prompt prior to the user inputting a password in response to the prompt.

5. (Previously Presented) The method of claim 4, wherein making the authentication graphic known comprises physically attaching the authentication graphic to the client.

6. (Currently Amended) The method of claim 1, further comprising:
receiving the password from the user;
generating a digest with a cryptographically-safe function using that includes indicia of the received password and the received password challenge, wherein the digest is a communication that securely protects the password from being intercepted; and
sending the digest to the server, wherein the server verifies the digest by comparing it to a recalculated digest that includes an indicia of the password challenge and a stored authentic password.

7. (Currently Amended) The method of claim 31, wherein the secret becomes stored in the secure storage when first entered by the user.

8. (Currently Amended) The method of claim ~~31~~, wherein the secret becomes stored in the secure storage when generated based upon information entered by the user.

9. (Currently Amended) A client device comprising:

a secure storage to store a secret;

a communications device to receive a password challenge from a server;

and

a secure password prompt authentication—routine embodied in the communications device to₁ in response to the password challenge, execute a procedure, wherein the procedure comprises:

(1) accessing ~~access~~—the secret in the secure storage, wherein the secret is a string of bits indicating colors and patterns for constructing the authentication graphic;

(2) generating ~~generate~~—an authentication graphic based on the secret[.]; and

(3) display-rendering a prompt-asking a user for a password at a display device, the prompt including a request for a user to input a password and the authentication graphic,₁ which ~~is~~are visible to the user,

wherein the secure password prompt routine ~~displays—renders the authentication graphic for all password challenges; there being no requirement of an association between the server and the authentication graphic;~~ and

a display device to present the rendered prompt to the user such that the authentication graphic of the presented prompt is recognized by the user as being associated with a secure request to input the password; and

a hash function embodied on the communications device to calculate a digest, wherein calculating comprises:

(1) receiving a password in response to the received password challenge, wherein the password is received upon the user identifying the authentication graphic as authentic;

(2) altering the password such that, if the digest is captured by an attacker, the attacker is unable to recreate the password; and

(3) calculating the digest from the password challenge and the altered password.

10-12. (Cancelled)

13. (Previously Presented) The client device of claim 9 wherein the authentication graphic is included on a body of the client device.

14. (Cancelled)

15. (Currently Amended) A machine-readable medium having stored thereon data representing instructions that, when executed by a processor of a client, cause the processor to perform operations comprising:

receiving a password challenge from a server;

responsive to the password challenge calling, a secure password prompt routine ~~which to execute a procedure, wherein the procedure comprises:~~

~~(1) accessing accesses~~ the secret in the secure storage[.];

~~(2) generating generates~~ an authentication graphic based on the secret[.]; and

~~(3) displays rendering~~ a prompt asking a user for a password at a display device, the prompt including a request for a user to input a password and the authentication graphic, which is are visible to the user; wherein the secure password prompt routine ~~displays renders~~ the authentication graphic for all password challenges, ~~there being no requirement of an association between the server and the authentication graphic.~~

16-17. (Cancelled)

18. (Previously Presented) The method of claim 15, further comprising making the authentication graphic known to the user so that the user can identify the authentication graphic on the prompt prior to the user inputting a password in response to the prompt.

19. (Previously Presented) The method of claim 15, wherein making the authentication graphic known comprises physically attaching the authentication graphic to the client.

20. (Currently Amended) The method of claim 15, further comprising:

receiving the password from the user;

altering the received password utilizing a hash function;

generating a digest using the ~~received~~ altered password and the received password challenge; and

sending the digest to the server without directly passing the password over a communications medium.

21. (Previously Presented) The method of claim 1, wherein making the authentication graphic known comprises including the authentication graphic in a user manual for the client.

22. (Previously Presented) The method of claim 1, wherein the authentication is unique to the client.